

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY**

**BOBBI POLANCO,**  
on behalf of herself and all  
others similarly situated,

Civil Action No. \_\_\_\_\_

Plaintiff,

v.

**OMNICELL, INC.; SOUTH JERSEY  
HEALTHCARE, INC.; SENTARA  
HEALTHCARE, INC.; UNIVERSITY OF  
MICHIGAN HEALTH SYSTEMS, INC;  
DOE'S 1-50; ABC Corporations 1-50; and  
XYZ Partnerships and Associations 1-50.**

**JURY TRIAL DEMANDED**

Defendants.

**CLASS ACTION COMPLAINT**

**TABLE OF CONTENTS**

<b>NATURE OF THE CASE.....</b>	<b>1</b>
<b>JURISDICTION AND VENUE.....</b>	<b>2</b>
<b>THE PARTIES.....</b>	<b>4</b>
Plaintiff.....	4
Defendants.....	5
<b>FACTUAL BACKGROUND.....</b>	<b>7</b>
<b>CLASS ACTION ALLEGATIONS.....</b>	<b>12</b>
<b><u>COUNT I</u> - BREACH OF STATE SECURITY NOTIFICATION LAWS.....</b>	<b>15</b>
<b><u>COUNT II</u> - VIOLATIONS OF THE NEW JERSEY, VIRGINIA AND MICHIGAN             CONSUMER FRAUD LAWS .....</b>	<b>18</b>
<b><u>COUNT III</u> – FRAUD .....</b>	<b>19</b>
<b><u>COUNT IV</u> - NEGLIGENCE.....</b>	<b>21</b>
<b><u>COUNT IV</u> - CONSPIRACY.....</b>	<b>22</b>
<b>PRAYER FOR RELIEF.....</b>	<b>24</b>
<b>JURY DEMAND.....</b>	<b>25</b>

Bobbi Polanco (“Plaintiff”), on her own behalf and on behalf of the Class, by and through her attorneys, alleges as follows:

**NATURE OF THE CASE**

1. This case is brought by Plaintiff who had her personal identifying and financial information accessed and then stolen without her authorization as a result of the negligence, unfair and deceptive acts and practices and unconscionable business practices of the Defendants.

2. On November 14, 2012, a laptop computer believed to be owned by Defendant, Omnicell, Inc., was stolen out of an employee’s car. The laptop contained Personal Confidential Information (“PCI”) of the Plaintiff and thousands of others who, like her, presented such information to various medical institutions in New Jersey and other States in conjunction with seeking healthcare treatment for themselves and/or their loved ones.

3. While it is not known exactly all of the PCI that was included on the laptop computer, the following categories of PCI were provided by those seeking healthcare at the Defendant hospitals:

- a. the names of patients, their relatives, and the parties responsible for payment of medical expenses;
- b. their addresses (including email addresses);
- c. their phone numbers (including unlisted phone numbers);
- d. their Social Security numbers;
- e. their financial account information (including banking, credit cards, and other financial account numbers);
- f. their employer and income information; and

- g. health information about their medical care and treatment at medical facilities covered by Health Insurance Portability and Accountability Act of 1996.

4. Despite the fact that the theft took place on November 14, 2012, the Defendants deliberately delayed in notifying Plaintiff and the Class about such breach. Had they provided timely notice of the breach in accordance with the data breach notification laws of New Jersey and the other States in which the Class members reside, Plaintiff and the Class could have and would have taken steps to protect themselves. Instead, for reasons unknown to Plaintiff and the Class, but unrelated to any requirements of law enforcement, Defendants chose to wait on until the earliest date of December 31, 2012 to tell people, by mail, about the incident.

5. Such deliberate and/or grossly negligent conduct, in the face of a preventable event had the Defendants taken appropriate steps to secure the PCI, including health information of Plaintiff and the Class, is actionable under the statutes and common law of New Jersey and the other States where members of the Class reside.

6. The case seeks to remedy the harmful effects of the breach of the privacy interests of Plaintiff and the Class, the failure to timely and reasonably notify them of such breach in accordance with the law, and the misleading and deceptive notification sent on December 31, 2012.

### **JURISDICTION AND VENUE**

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and 1332(d), because the matter in controversy exceeds \$5 million exclusive of interest and costs, and because more than

two-thirds of the members of the putative Class are citizens of states different from that of the Defendants named in this lawsuit.

8. Under 28 U.S.C. § 1391, venue is proper in this District because Defendants engaged in substantial conduct relevant to the claims Plaintiff, and caused harm to Plaintiff and the Class. A substantial part of the events or omissions giving rise to the claims in this action occurred in this judicial District, and at least one of the Defendants may be found within this judicial District.

9. This Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over the Plaintiff's allegations of violations of the state security notification and consumer protection laws of the State of New Jersey and other States, as well as claims of common law fraud, negligence and civil conspiracy/concert of action.

10. This Court has personal jurisdiction over the parties because the Defendants conduct substantial business in this State, have had systematic and continuous contacts within this State, and have agents and representatives that can be found in this State.

11. The Court has jurisdiction over the individual Defendants because they have had sufficient minimum contacts with and/or have purposefully availed themselves of the laws and markets of the State of New Jersey through, among other things, their conspiratorial communications between themselves and with others (including telephonic and electronic communications) and their receipt, marketing, sale and/or distribution of the PCI of residents of New Jersey and other States.

## **THE PARTIES**

### **Plaintiff**

12. Plaintiff, Bobbi Polanco, is an individual and resident of New Jersey residing at 564 Landis Avenue, Bridgeton, New Jersey. As discussed more fully below, Mrs. Polanco had her PCI accessed without her authorization on or about November 14, 2102. More than six (6) weeks later, Mrs. Polanco first received notice of the theft of her PCI in a letter from Defendant, Omnicell, Inc., informing her that her PCI had been accessed without authorization. A true and correct copy of the December 31, 2012 letter is attached hereto as Exhibit "A". At no time had Mrs. Polanco received any communication from Defendant, South Jersey Healthcare, Inc., regarding this incident. Since the subject data breach, Mrs. Polanco has paid hundreds of dollars in securing medical care and treatment for her daughter at medical facilities far more remote than the facilities within South Jersey Healthcare system where she previously took her daughter for treatment. Ms. Polanco is unwilling to return to South Jersey Healthcare until such time as her PCI is secure, her rights under the Health Insurance Portability and Accountability Act of 1996 are protected, and the deficiencies that led to the November 14 incident have been corrected to her satisfaction.

13. As discussed throughout this Complaint, Plaintiff suffered direct injury and damages as a result of the data breach and compromise of her PCI, the negligence of Defendants, and the acts and omissions and unlawful conduct of the Defendants set forth herein.

**Defendants**

14. Omnicell, Inc. (“Omnicell”) is Delaware corporation with its corporate headquarters at 1201 Charleston Road, Mountain View, California 94043.

15. Omnicell sells automation and analytics solutions designed to enable healthcare facilities to acquire, manage, dispense and administer medications and medical-surgical supplies. Its systems provide medication control and dispensing starting from the point of entry into the hospital and other health care providers, through the central pharmacy, to the nursing station and to the patient’s bedside. Omnicell’s medication-use product line includes its OmniRx, SinglePointe, AnywhereRN, Anesthesia Workstation, WorkflowRx, Controlled Substance Management, OmniLinkRx, Savvy Mobile Medication System, and Pandora Data Analytics products.

16. Omnicell has satellite locations in Illinois and Dubai. Omnicell’s products are in more than 2,500 healthcare facilities and its revenue in 2011 was in excess of \$245 million.

17. Defendant, South Jersey Healthcare (“SJH”), is a non-profit healthcare organization headquartered at 1505 West Sherman Street, Vineland, New Jersey.

18. SJH owns and maintains two hospitals. The SJH Regional Medical Center, the system’s newest hospital, is a 262-bed facility located in Vineland, New Jersey. The SJH Elmer Hospital is a 96-bed facility located in Elmer, New Jersey. SJH also provides offers outpatient care in more than 40 locations. Until being notified about the theft of her PCI described herein, Plaintiff brought her daughter to SJH healthcare facilities for medical care and treatment.

19. Defendant, Sentara Healthcare (“Sentara”), is a non-profit healthcare organization with its headquarters at 6015 Poplar Hall Drive, Norfolk, Virginia 23502.

20. Sentara owns and operates at least twelve (12) hospitals, including Sentara CarePlex, Sentara Leigh Hospital, Sentara Norfolk General Hospital, Sentara Obici Hospital, Sentara Princess Anne Hospital, Sentara Virginia Beach General Hospital, Sentara Williamsburg Regional Medical Center, Sentara Belle Harbor Hospital, Sentara Independence Hospital, Sentara Port Warwick Hospital, Sentara Northern Virginia Medical Center and the Martha Jefferson Hospital.

21. Defendant, University of Michigan Health System (“UMHS”), is the wholly owned academic medical center of the University of Michigan with its headquarters at 1500 East Medical Center Drive, Ann Arbor, Michigan.

22. In a typical year, the UMHS has over 1.8 million outpatient and emergency visits, 44,000 hospital stays, 46,000 surgeries and 4,000 births at its facilities.

23. Defendants Doe’s 1-50, ABC Corporations 1-50 and XYZ Partnerships and Associations (collectively “the Doe Defendants”) are persons and entities who may have received the PCI of Plaintiff and the Class. The identities and locations of the Doe Defendants are not yet known, but may be knowable in the future once the investigation of others is complete.

24. All the foregoing defendants are collectively referred to herein as “Defendants.” SJH, Sentara and UMHS are collectively referred to herein as “the Hospital Defendants.”

25. The acts alleged in this Complaint to have been done by each of the Defendants were authorized, ordered, done and/or ratified by their respective officers,



directors, agents, employees or representatives while engaged in the management, direction, control or transaction of their respective business affairs.

26. Various persons and/or firms not named as Defendants herein, have participated as co-conspirators in the violations alleged herein and have performed acts and made statements or omissions in furtherance thereof.

### **FACTUAL BACKGROUND**

27. Mrs. Polanco first moved to the Vineland area in November 2011 so that she and her husband could provide a better life for themselves and minor their daughter, who is now six (6) years old.

28. Since moving to the Vineland area, the Polancos' daughter has suffered from a series of medical events, including upper respiratory infections, bronchitis, fevers and episodes where her throat swells making it difficult for her to breath.

29. Mrs. Polanco has taken her daughter to both the SJH Regional Medical Center and the Elmer Hospital owned by SJH at least five (5) times since 2011.

30. During each of her visits to SJH hospitals, the Polancos' daughter has been treated in the emergency room given the sudden on-set of her symptoms.

31. Given the suddenness of her illnesses and her readily apparent distress in breathing, it has been Mrs. Polanco's goal to get her daughter to the closest hospital to seek treatment for her daughter as quickly as possible.

32. During those visits to the SJH hospitals, the Polancos' daughters' treatment has included antibiotics administered intravenously.

33. During Mrs. Polanco's first visit to the SJH hospitals, she provided SJH with her Social Security Number, her insurance information, her and her daughters' date

of birth, a summary of the medical condition giving rise to the hospital visit among other information. During each subsequent visit, Mrs. Polanco confirmed the accuracy of the previously provided information as well as provided a summary of the medical condition giving rise to the current hospital visit.

34. During her visits to SJH, Mrs. Polanco was also provided with a copy of SJH's privacy policy indicating that SJH would take appropriate measures to safe-guard her and her daughter's PCI. The representation of SJH that it would safeguard the privacy of her PCI was one of the reasons why she opted to visit the SJH hospitals.

35. As stated in a December 31, 2012 letter from Omnicell, on the night of November 14, 2012, "an Omnicell electronic device issued to an Omnicell employee was stolen from his locked car." *See* Exhibit "A".

36. Based upon media reports, the electronic device stolen from the Omnicell employee's car was a laptop computer and the PCI data on the laptop was not encrypted.

37. The failure to encrypt the PCI constitutes as violation of the Health Insurance Portability and Accountability Act of 1996, as discussed below.

38. The laptop computer contained the unencrypted PCI of Mrs. Polanco and her daughter, plus the unencrypted PCI of thousands of other individuals including the following types of information:

- a. The name of the patient, their birth date, patient number, and medical record number;
- b. The gender of patient;
- c. Allergies of the patient;
- d. The admission and/or discharge date(s) of the patient;
- e. The name of the patient's physician;

- f. Their patient type (*i.e.*, inpatient, emergency department or outpatient);
- g. The site and area of the hospital which treated the patient (*e.g.*, specific inpatient or outpatient unit/area);
- h. The room number of the patient;
- i. The name(s) of medication(s) used to treat the patient, along with all the following related information: the dosage amount, rate, route (*e.g.*, oral, infusion, etc.), frequency, administration instructions, and start/stop times.

39. Although the December 31, 2012 Notice Letter provided certain information about the theft of the PCI of Plaintiff and the Class, it failed to advise Plaintiff and the Class about the material information concerning the loss of their PCI, such as how and why an Omnicell employee came to have in his possession, outside a medical facility, an Omnicell laptop computer containing PCI of Plaintiff and the Class; how and why the PCI was unencrypted, in violation of the Health Insurance Portability and Accountability Act of 1996; and what concrete steps were being taken by all Defendants to secure existing PCI to ensure that the PCI of Plaintiff and the Class was not compromised in the future.

40. The delay between the November 14, 2012 theft and the December 31, 2012 Letter by Omnicell was unreasonable and was not mandated by law enforcement.

41. According to media reports, tens of thousands of patients were affected by the Omnicell data breach including 8,500 patients from SJH; 4,000 from UMHS; and 56,000 from Sentara.

42. Since receiving the December 31, 2012 Notice Letter from Omnicell, and because she has received no reassurance from the Defendants that they are taking the necessary steps to ensure that her PCI is safe from subsequent loss by the Defendants and

unauthorized access, Plaintiff has opted to seek treatment for her daughter from hospitals that are not a part of SJH. For example, on January 23, 2013, as a direct result of the loss of her PCI by SJH, Mrs. Polanco took her daughter to The Memorial Hospital of Salem County in Salem, New Jersey, as opposed to either the SJH Regional Medical Center in Vineland or the Elmer Hospital in Elmer, New Jersey. The Memorial Hospital of Salem County is 23.6 miles from Mrs. Polanco's home whereas SJH Regional Medical Center is 8.2 miles from Mrs. Polanco's home and Elmer Hospital is 13.3 miles from her home.

43. The reasonable actions of Mrs. Polanco to seek treatment for her daughter at the Memorial Hospital of Salem County has resulted in increased costs for Mrs. Polanco to seek treatment for her daughter. It is believed and therefore averred that additional Class members have incurred, and continue to incur, additional expenses by seeking care at alternative hospitals following the data breach described in the December 31, 2012 Notice Letter.

44. Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the U.S. Department of Health and Human Services ("HHS") issued the Standards for Privacy of Individually Identifiable Health Information ("the Privacy Rule"). The Privacy Rule was effective December 28, 2000.

45. The Privacy Rule was implemented to protect all individually identifiable health information which is defined by the Privacy Rule as Protected Health Information ("PHI").

46. Pursuant to the Privacy Rule, SJH, Sentara and UMHS are Health Care Providers and are, therefore, "Covered Entities" under the Privacy Rule.

47. Omnicell is a "Business Associate" under the Privacy Rule.

48. Under the Privacy Rules, Covered Entities must have written agreements with Business Associates, known as Business Associate Agreements, if PHI is given to the Business Associate by the Covered Entities.

49. In the Business Associate Agreement, the Covered Entity must impose specified written safeguards to protect the privacy of a patient's PHI used by or disclosed to a Business Associate.

50. Pursuant to the Privacy Rule, a Covered Entity must make reasonable efforts to use, disclose and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure or request and must develop and implement policies and procedures to limit the use and disclosure of PHI to the minimum necessary. 45 C.F.R. § 164.502(b).

51. A Covered Entity also is required to mitigate any harmful effects it learns were caused by the use or disclosure of PHI by its workforce or Business Associates in violation of the Privacy Rule. 45 C.F.R. § 164.530.

52. The Privacy Rule requires that Covered Entities take specific actions upon learning of a breach of unsecured PHI including requirements that the Covered Entity notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired used or disclosed as a result of such breach. 45 C.F.R. § 164.404(a)(1).

53. A Covered Entity is required to provide notification of a breach "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." 45 C.F.R. § 164.404(b).

54. The notice must include the following: (a) a brief description of what happened including the date the breach was discovered; (b) a description of the types of PHI that was involved in the breach; (c) any steps the individuals should take to protect themselves from harm arising from the breach; (d) a description of what the Covered Entity is doing to investigate and mitigate harm to the individuals; and (e) contact procedures to learn more information including a toll-free telephone number, an e-mail address, Web site or postal address. 45 C.F.R. § 164.404(c).

55. In the event that a breach of unsecured PHI involves more than 500 residents of a State, a Covered Entity is required to notify prominent media outlets of the breach. 45 C.F.R. § 164.406.

56. If a Business Associate learns of a breach, it must notify the Covered Entity of the breach without unreasonable delay, but in any event no later than 60 days following the breach. 45 C.F.R. § 164.410.

57. A Covered Entity is in violation of the Privacy Rule if it knows of a pattern of activity or practices by a Business Associated that constituted a breach or violation of the Business Associate's obligations under its contract with the Covered Entity unless the Covered Entity took reasonable steps to cure the breach or end the violation or terminated the contract or agreement if such to cure the breach were unsuccessful. 45 C.F.R. § 164.504(e).

#### **CLASS ACTION ALLEGATIONS**

58. Plaintiff and the Class hereby incorporate by reference thereto the preceding and following paragraphs hereof as if fully set forth herein.

59. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of herself, and on behalf of all individuals who had their PCI stolen from the electronic device issued to the Omnicell employee on the evening of November 14, 2012.

60. Plaintiff also seeks certification of a Class pursuant to Fed. R. Civ. P. 23(b)(2) as Plaintiff seeks declaratory and injunctive relief.

61. The Class consists of numerous individuals and entities throughout the United States, making individual joinder impractical, in satisfaction of Rule 23(a)(1).

62. The disposition of the claims of the Class members in a single class action will provide substantial benefits to all parties and to the Court.

63. The claims of the representative Plaintiff are typical of the claims of the Class, as required by Rule 23(a)(3), in that the representative Plaintiff had her PCI stolen on the evening of November 14, 2012 and has thereafter suffered damage as a proximate result.

64. The factual and legal bases of each of the Defendants' misconduct are common to the Class Members and represent a common thread of fraud and other misconduct resulting in injury to Plaintiff and the members of the Class.

65. There are many questions of law and fact common to the Plaintiff and the Class, and those questions predominate over any questions that may affect individual Class Members, within the meaning of and fulfilling the requirements of Rules 23(a)(2) and 23(b)(2) and (3). Common questions of law and fact include, but are not limited to, the following:

- a. Whether the Defendants complied with the data breach notification laws of New Jersey, Virginia and Michigan;

- b. Whether the Defendants' conduct was consistent with the requirements of the HIPAA Privacy Rules;
- c. Whether the Defendants complied with HIPAA's requirements concerning Business Association Agreements;
- d. Whether the Defendants properly notified the Class of the November 14, 2012 data breach;
- e. Whether the Defendants took proper steps to mitigate the potential damage to the Class arising from the November 14, 2012 data breach;
- f. Whether the Hospital Defendants' decision to abdicate their responsibility to notify the Class of the November 14, 2012 data breach to Omnicell was proper under the applicable laws and regulations.

66. Plaintiff will fairly and adequately represent and protect the interests of the Class, as required by Rule 23(a)(4). Plaintiff has retained counsel with substantial experience in prosecuting nationwide consumer class actions. Plaintiff and their counsel are committed to vigorously prosecuting this action on behalf of the Class, and have the financial resources to do so. Neither Plaintiff nor her counsel has any interest adverse to those of the Class.

67. Plaintiff and members of the Class have all suffered, and will continue to suffer, harm and damages as a result of the Defendants' unlawful and wrongful conduct.

68. A class action is superior to other available methods for the fair and efficient adjudication of this controversy under Rule 23(b)(3). Absent a class action, most members of the Class likely would find the cost of litigating their claims to be prohibitive, and will have no effective remedy at law.



69. The class treatment of common questions of law and fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the Court and the litigants, and promotes consistency and efficiency of adjudication.

70. The Defendants have acted and failed to act on grounds generally applicable to Plaintiff and the Class and require that the Court impose uniform relief to ensure compatible standards of conduct toward the Class, thereby making appropriate equitable relief to the Class as a whole within the meaning of Rules 23(b)(1) and (b)(2).

**COUNT I**  
**BREACH OF STATE SECURITY NOTIFICATION LAWS**

71. Plaintiff hereby incorporates by reference the preceding paragraphs as if fully set forth here and further alleges as follows.

72. Upon information and belief, Defendants first knew, or should have known, that the PCI of the Plaintiff and the Class had been stolen on the night of November 14, 2012.

73. Defendant Omnicell waited a full forty-seven (47) days to issue letter to Plaintiff (and presumably other members of the Class) about the theft.

74. Defendant SJH has never notified Plaintiff or members of the Class of the theft.

75. At least forty-four States, the District of Columbia and Puerto Rico have enacted legislation requiring notification of security breaches involving personal information, including but not limited to the states of New Jersey, N.J. Stat. 56:8-163, Virginia, VA Code Ann. § 18.2-186.6, and Michigan, M.C.L.A. 445.72.

76. By the acts and omissions set forth herein, Defendants have violated security breach notification laws of New Jersey, Virginia, Michigan and the other states where members of the Class reside.

77. The New Jersey law, N.J. Stat. 56:8-163, specifically provides that:

Any business that conducts business in New Jersey ... **shall disclose** any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made **in the most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. ...

\* \* \*

Any business ... required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.

The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.

N.J.S.A. 56:8-163.

78. As described in detail above, Defendants failed to comply with these statutory requirements, and similar requirements under other States' laws by, *inter alia*, failing to disclose "in the most expedient time possible and without unreasonable delay",

in the case of Defendant, Omnicell, the fact of the breach of PCI of Plaintiff and the Class.

79. In the case of Defendant SJH, there has been no disclosure to date.

80. It is believed and therefore averred that “the legitimate needs of law enforcement” did not prevent any Defendant from providing expedient notice to Plaintiff and the Class. Specifically, it is believed and therefore averred that a law enforcement agency did not “determine[] that the notification will impede a criminal or civil investigation” and did not make “a request that the notification be delayed” until December 31, 2012, when Defendant Omnicell sent a letter to Plaintiff.

81. To the contrary, because the theft did not occur in New Jersey, it is highly unlikely any New Jersey law enforcement agency impeded compliance with the law by Defendants.

82. It is also believed, and therefore averred, that Defendants failed to, “in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling.”

83. Because the breach of PCI in this case involved more than 1,000 persons, Defendants were required to, but failed to, “also notify, without unreasonable delay, all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis, as defined by subsection (p) of section 603 of the federal ‘Fair Credit Reporting Act’ (15 U.S.C. s. 1681a), of the timing, distribution and content of the notices.”

84. New Jersey law also provides as follows:

“A business ... shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal

information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.”

N.J.S.A. 56:8-162.

85. To the extent Defendants were no longer required to retain the PCI of Plaintiff and the Class after the theft on November 14, 2012, Defendants violated New Jersey law.

86. Because New Jersey provides that violations of the foregoing statutes constitute unlawful practices within the meaning of the New Jersey consumer fraud law, the foregoing acts and failures to act by Defendants constitute *per se* violations of New Jersey law.

87. Defendants acted willfully, knowingly and/or recklessly with respect to their acts and omissions above.

**WHEREFORE**, Plaintiff respectfully seeks the relief set forth below.

**COUNT II**  
**VIOLATIONS OF THE NEW JERSEY,**  
**VIRGINIA AND MICHIGAN CONSUMER FRAUD LAWS**

88. Plaintiff hereby incorporates by reference the preceding paragraphs as if fully set forth here and further alleges as follows.

89. Plaintiff and the Class are actual consumers who provided Defendants with their PCI under the express representation that the same would not illegally be accessed, downloaded, saved, distributed, transferred and sold to various individuals and entities not yet fully known.

90. New Jersey, Virginia and Michigan have enacted laws to protect consumers against unfair, deceptive or fraudulent business practices, unfair competition and false advertising and unconscionable business practices.

91. New Jersey, Virginia and Michigan allow consumers a private right of action under such laws.

92. By the misrepresentations and non-disclosure of material facts alleged above, the Defendants deceived and continue to deceive consumers, such as Plaintiff and the Class. This conduct constitutes unconscionable, unlawful, unfair, deceptive and/or fraudulent business practices within the meaning of the New Jersey Consumer Fraud Act, 56:8-1, *et seq.*, The Virginia Consumer Protection Act, VA Code Ann. § 59.1-196 *et seq.*, and the Michigan Consumer Protection Act, M.C.L.A. 445.901 *et seq.*

93. As a direct and proximate result of the Defendants' unfair and deceptive trade practices, Plaintiff and the Class have and will continue to suffer damages in an amount to be determined at trial.

**WHEREFORE**, Plaintiff respectfully seeks the relief set forth below.

**COUNT III**  
**FRAUD**

94. Plaintiff hereby incorporates by reference the preceding paragraphs as if fully set forth here and further alleges as follows.

95. By engaging in the acts and omissions alleged in this Complaint, Defendants have committed fraud on the Plaintiff and the Class.

96. Defendants have made false and fraudulent statements and material misrepresentations and omissions to Plaintiff and the Class relating to the receipt, storage, maintenance and privacy of their PCI, as well as the time, place and manner of the unauthorized access to their PCI. Defendants' statements were misleading, at best, and materially false and fraudulent, at worst.

97. Defendants intended that Plaintiff and the Class would rely on their statements, representations and omissions to their detriment. In particular, the Defendants made misrepresentations about the security of the PCI they sought and received from Plaintiff and the Class. Then, after the breach, they failed to timely notify Plaintiff and the Class of the breach, as required by law. Plaintiff and the Class have relied on Defendant's misrepresentations to their detriment.

98. In addition, the Defendants concealed and suppressed and/or omitted material facts as to their knowledge of the unauthorized access PCI.

99. As a result of the Defendants' acts of concealment and suppression, and their misrepresentations and omissions, Plaintiff and the Class were unaware of the facts of the data breach for more than 47 days, and thus, were unable to take timely action to protect themselves from the harmful effects of the unauthorized disclosure of their PCI.

100. As a direct and proximate result of Defendants' fraudulent representations and omissions, and the concealment and suppression of material facts by Defendants, Plaintiff and the Class have suffered and will continue to suffer damages.

**WHEREFORE**, Plaintiff respectfully seeks the relief set forth below.

**COUNT IV**  
**NEGLIGENCE**

101. Plaintiff hereby incorporates by reference the preceding paragraphs as if fully set forth here and further alleges as follows.

102. The Defendants, as recipients of the PCI of Plaintiff and the Class owed a duty of care to Plaintiff and the Class to ensure that their PCI was properly protected and safe from unauthorized disclosure to third parties.

103. The Defendants' conduct failed to comply with their duty of care by allowing the PCI of Plaintiff and the Class to be stored on a laptop in an unencrypted format.

104. The Defendants' conduct failed to comply with applicable regulations, including HIPAA regulations.

105. The Defendants' conduct in failing to protect the security of the PCI of Plaintiff and the Class was a breach of their duty of care.

106. The Defendants' conduct in failing to timely notify Plaintiff and the Class of the breach of security concerning their PCI was a breach of their duty of care.

107. The Defendants' conduct in failing to mitigate the potential of harm arising from the breach of security concerning their PCI was a breach of their duty of care.

108. The Hospital Defendants' failure to ensure that Defendant Omnicell's data protection measures were in compliance with HIPAA regulations was a breach of their duty of care to Plaintiff and the Class.

109. The Hospital Defendants' failure to ensure that Defendant Omnicell was compliant with the data protection measures required by their Business Association Agreement as required by HIPAA was a breach of their duty of care to Plaintiff and the Class.

110. All of the failures of the Defendants to exercise reasonable care were the proximate cause of harm to Plaintiff and the Class.

111. Plaintiff and the Class each suffered damages as a result of the Defendants' breach of the applicable standards of care.

**WHEREFORE**, Plaintiff and the Class respectfully seek the relief set forth below.

**COUNT IV**  
**CONSPIRACY**

112. Plaintiff hereby incorporates by reference the preceding paragraphs as if fully set forth here and further alleges as follows.

113. As set forth more fully above, beginning at least as early as November 15, 2102, the exact date being unknown to Plaintiff and the Class, and continuing thereafter, Defendants and their co-conspirators entered into an agreement and/or otherwise engaged in a continuing conspiracy to defraud the Plaintiff and the Class by causing PCI of Plaintiff and the Class to be stolen and acting in their own interests and to the detriment of Plaintiff and the Class by failing to timely notify Plaintiff and the Class of the loss of their PCI.

114. Pursuant to the widespread conspiracy alleged herein and in furtherance thereof, Defendants and their co-conspirators engaged in a wide range of activities, the purpose and effect of which was to defraud the Plaintiff and to act or take substantial



steps in furtherance of the conspiracy. Upon information and belief, those activities include the following:

- a. Defendants discussed and agreed among themselves and with their co-conspirators that they would allow Defendant Omnicell to possess unencrypted the PCI of Plaintiff and the Class;
- b. Defendants discussed and agreed among themselves and with their co-conspirators that they would not alert Plaintiff and the Class of the loss of the PCI in a timely manner;
- c. Defendants discussed and agreed among themselves and with their co-conspirators that the Hospital Defendants would not alert Plaintiff and the Class to the loss of the PCI and, instead, would delegate to Defendant Omnicell the obligation to notify Plaintiff and the Class of the loss of the PCI;
- d. Defendants discussed and agreed among themselves and with their co-conspirators that they would not take steps to mitigate the damage to Plaintiff and the Class resulting from the loss of the PCI;
- e. Defendants discussed and agreed among themselves and with their co-conspirators that they would not offer Plaintiff and the Class any assistance in the monitoring of their credit profiles following the loss of the PCI.

115. Defendants performed these acts alleged herein in furtherance of the common plan or design for the conspiracy with knowledge of the injury and damage it would cause to Plaintiff and the Class and with intent to cause such injuries or with reckless disregard for the consequences.

116. As a direct and proximate result of Defendants' conspiracy as alleged herein, Plaintiff and the Class have been injured and damaged, and Defendants are jointly and severally liable for such injuries and damages.

**WHEREFORE**, Plaintiff respectfully seeks the relief set forth below.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff and the Class request that the Court Order the following relief:

- a. Declare unlawful the acts and practices alleged herein, and enjoin the Defendants from committing the acts complained of herein;
- b. Enter judgment against all Defendants for the violations alleged herein;
- c. Award the actual damages incurred by Plaintiff as a result of the wrongful acts complained of, along with pre-judgment and post-judgment interest at the maximum rate allowed by law;
- d. Award statutory damages set forth herein;
- e. Award of treble damages or multiple damages by operation of law;
- f. Award punitive damages;
- g. Award Plaintiff the costs of this action, including reasonable attorney's fees, and, where applicable, expert fees; and
- h. Award such other and further relief as the Court may deem just and appropriate.

**JURY DEMAND**

Plaintiff demands a trial by jury of all issues so triable in this cause.

Respectfully submitted,

Dated: March 8, 2013


/s/ Mark L. Rhoades  
Donald E. Haviland, Jr., Esquire  
Mark L. Rhoades, Esquire  
Christina M. Philipp, Esquire  
Haviland Hughes  
112 Haddontowne Court  
Suite 202  
Cherry Hill, NJ 08034  
856-354-0030 Telephone

**ATTORNEYS FOR PLAINTIFF,  
BOBBI POLANCO AND THE CLASS**

# **EXHIBIT A**



December 31, 2012

1L-88716-LV4-0000129 T-0001 \*\*\*\*\*5-DIGIT 0830  
 BOBBI POLANCO  
 43 PRESTON AVE  
 BRIDGETON, NJ 08302-1464  


RE: VALENTINA POLANCO

Dear Parent/Personal Representative of Valentina Polanco:

Omnicell, Inc. ("Omnicell") provides automated medication dispensing services on behalf of various healthcare providers, including South Jersey Healthcare ("South Jersey Hospital"). In providing these services, Omnicell is entrusted with patient information. Omnicell takes our obligation to protect patient information seriously. Regrettably, we are writing to inform you about an incident involving health information about the above-named patient, for whom we have you listed as the parent or personal representative.

On the night of November 14, 2012, an Omnicell electronic device issued to an Omnicell employee was stolen from his locked car. We became aware of the incident on November 15, 2012. The incident was reported to the police, and we immediately began a thorough investigation to identify the information that was contained on the device. To date, the device has not been located. Omnicell advised South Jersey Hospital of the incident on November 20, 2012.

Our investigation shows the files on the device could have contained the following information about the patient:

Patient name, birth date, patient number, and medical record number.

Additionally, one or more of the following clinical information may have been involved:

Gender, allergies, admission date and/or discharge date; physician name; patient type (i.e., inpatient, emergency department or outpatient); site and area of the hospital (e.g., specific inpatient or outpatient unit/area); room number; medication name; and medication dose amount and rate, route (e.g., oral, infusion, etc.), frequency, administration instructions, and start time and/or stop time.

A sample copy of what the patient-specific data would actually look like on the device is shown below:

```
Incoming command: Que Body{SVR BRBIBC PMI \pmdt:2012110400434700\uid:
:[EmployeeUserUniqueId]\pid:[0123456789]\item:7402009\pmt:S\ui:EA\dssu:MG\pmm:\pml:\pml:N\p
mi:30.0000\pma:0.0000\pmc:0.0000\pmw:0.0000\pmr:0.0000\pmint:30.0000\pmew:0.0000\pmnd:\p
mud:30.0000\pmun:0.0000\una:[Employee Name]\pna:[Patient Name]\ina:[Medication
Name]\rs:30MG
TAB\acv:3\jgc:G\res:N\wstrq:Y\rw:N\rcd:Y\pkd:30.0000\pmab:N\pmac:30.0000\lsti:201211040043470
0\lsto:BRER\lsta:BER\lstd:2012110400434700\mu:N\mdc:N\mdy:N\pms:R\lud:2012110400453964\luf:S
VR\lmoid:\lprn:\ismix:N\cyrcq:N\luu:\radt:N) TD:0s PD:0s
```

(OVER PLEASE)

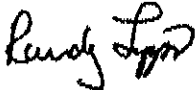
1L-88716-LV4

The patient's medical records were not on the device, and the patient's medical information has not been lost. Also, the patient's financial information, bank account information, Social Security number, and insurance information were not on the device.

Omniceil has no reason to believe that the device was taken for the information it contained, or that the information has been accessed or used improperly. However, we wanted to notify you and assure you that we are taking this matter seriously. Moreover, as a precautionary measure, we recommend that you monitor medical insurance statements for any evidence of fraudulent transactions using the patient's identity. If you suspect any fraudulent transactions have occurred, you should contact your local law enforcement agency or the state attorney general.

We deeply regret any concern this may cause you. Omnicell is continuing to investigate this incident and is working closely with local authorities to locate the stolen device and secure all patient information. Moreover, Omnicell is taking steps to improve its security program and practices in response to this incident. We have assured South Jersey Hospital that we have taken steps, including technology changes and re-education of our employees, to assure that no patient information is stored on unsecured electronic devices in the future. If you have any questions, please call 1-855-755-8483, Monday through Friday between 8 a.m. and 5 p.m. Eastern time. When prompted, please enter the following 10-digit reference number: 6239121712.

Sincerely,



Randy Lipps  
CEO  
Omnicell